

Classical simulatability of the one clean qubit model

Tomoyuki Morimae^{1,*} and Takeshi Koshihara²

¹*ASRLD Unit, Gunma University, 1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan*

²*Graduate School of Science and Engineering, Saitama University,
255 Shimo-Okubo, Sakura, Saitama 338-8570, Japan*

(Dated: June 6, 2014)

Deterministic quantum computation with one quantum bit (DQC1), or the one clean qubit model, [E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998)] is a model of quantum computing where the input is the tensor product of a single pure qubit and many completely-mixed states, and only the single qubit is measured at the end of the computation. In spite of its naive appearance, the DQC1 model can efficiently solve some problems for which no classical efficient algorithms are known, and therefore it has been conjectured that the DQC1 model is more powerful than classical computing (under the assumption of $\text{BPP} \subsetneq \text{BQP}$). However, there has been no proof for the conjecture. Here we show that the output probability distribution of the DQC1 model cannot be classically efficiently approximated (exactly within a polynomial bit length or in the fully polynomial randomized approximation scheme (FPRAS) with at most a constant error) unless $\text{BQP} \subseteq \text{BPP}$.

I. INTRODUCTION

The deterministic quantum computation with one quantum bit (DQC1), or the one clean qubit model, proposed by Knill and Laflamme [1] is a restricted model of quantum computing. It was originally motivated by nuclear magnetic resonance (NMR) quantum information processing, but now it has been extensively studied in variety of contexts to understand the border between quantum and classical computing [3–13]. As shown in Fig. 1 (a), a DQC1 circuit consists of

1. the input state $|0\rangle\langle 0| \otimes \frac{I^{\otimes n}}{2^n}$, where $I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator,
2. a $\text{poly}(n)$ -size quantum gate U ,
3. the computational basis measurement of the first qubit, which gives the output bit $a \in \{0, 1\}$.

The DQC1 model seems to be very weak, and in fact, it does not support universal quantum computation under reasonable assumptions [2]. However, counter-intuitively, the DQC1 model can efficiently solve some problems for which no efficient classical algorithm is known, such as the spectral density estimation [1], testing integrability [3], calculation of fidelity decay [4], approximation of the Jones and HOMFLY polynomials [5–7] and an invariant of 3-manifolds [8]. These results are surprising since if we replace the single pure input qubit with the completely mixed qubit, then the output suddenly becomes trivially classically simulatable. In other words, the single pure qubit hides some capacity of unlocking the potential power of highly-mixed states for the quantum speedup. In fact, such an unexpected power of the DQC1 model was shown to come from some non-classical correlations between the mixed register and the pure qubit [9–11]. In short, the DQC1 model is believed to be a model

of computation which is intermediate classical and universal quantum computation.

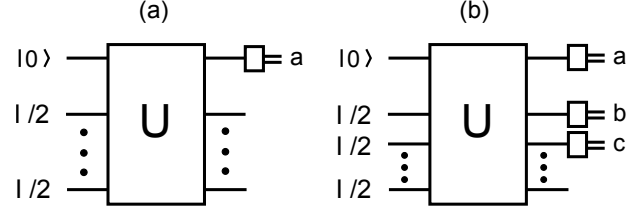


FIG. 1: (a) The DQC1 model. (b) The DQC1_m model for $m = 3$.

In Ref. [12], a generalized version of the DQC1 model, which is called the DQC1_m model, was introduced. The DQC1_m model is the same as the DQC1 model except that not a single but m output qubits are measured in the computational basis at the end of the computation (Fig. 1 (b)). In particular, the DQC1₁ model is equivalent to the DQC1 model. It was shown in Ref. [12] that the output probability distribution of the DQC1_m model for $m \geq 3$ cannot be classically efficiently sampled (within a multiplicative error) unless the polynomial hierarchy collapses at the third level [12]. The polynomial hierarchy [14] is a natural way of classifying the complexity of problems (languages) beyond the usual NP (nondeterministic polynomial time, which includes “traveling salesman” and “satisfiability” problems). Since it is believed in computer science that the polynomial hierarchy does not collapse, it is unlikely that the DQC1_m model for $m \geq 3$ can be classically efficiently sampled. This result is based on the “postselection technique” used for other restricted models of quantum computing, such as the depth-four circuits model by Terhal and DiVincenzo [15], the instantaneous quantum polytime (IQP) model by Bremner, Jozsa, and Shepherd [16], and the Boson sampling model by Aaronson and Arkhipov [17].

*Electronic address: morimae@gunma-u.ac.jp

Can we show an impossibility of classical efficient simulation of the DQC1_m model for $m \leq 2$? In particular, the case for $m = 1$, which corresponds to the original DQC1 model, has been the long standing open problem.

In this paper, we show that if we can classically efficiently approximate (exactly within a polynomial bit length or in the fully polynomial randomized approximation scheme (FPRAS) with at most a constant error) the output probability distribution of the DQC1 model, then $\text{BQP} \subseteq \text{BPP}$.

Although the belief of $\text{BPP} \subsetneq \text{BQP}$ is relatively less solid than the belief of $\text{P} \neq \text{NP}$ or that the polynomial hierarchy does not collapse, researchers in quantum computing believe $\text{BPP} \subsetneq \text{BQP}$ (for example, there is an oracle A relative to which $\text{BPP}^A \neq \text{BQP}^A$ [18]). Therefore our results suggest that DQC1 model can unlikely be classically efficiently simulated in these senses.

If we replace the single pure qubit $|0\rangle$ of the DQC1 model with the completely-mixed qubit I , the output probability distribution suddenly becomes easy to be classically calculated. Therefore, our results demonstrate “a power of a single qubit” in the DQC1 model. Furthermore, it is known that some quantum circuits, which look more complicated than the DQC1 model, such as the stabilizer circuits [19] and matchgates [20], can be classically efficiently simulated. These facts therefore suggest that the superficially naive DQC1 model indeed hides some ability of doing complicated quantum computing.

Note that definitions of classical simulatability considered in this paper are based on the calculation, and therefore stronger than the sampling, which was used in Refs. [12, 16]. It is still an open problem whether DQC1_m model for $m \leq 2$ is hard to be classically simulated in the sense of sampling.

II. FIRST RESULT

Let $P(a) : \{0, 1\} \rightarrow [0, 1]$ be the probability of obtaining the result $a \in \{0, 1\}$ in the computational basis measurement of the output qubit in the DQC1 model. Let $P'(a)$ be an approximation of $P(a)$:

$$0 \leq P(a) - P'(a) \leq \epsilon,$$

where $0 \leq \epsilon \leq \frac{1}{2^r}$ and r is a polynomial of n sufficiently larger than $n - 1$. If there exists a deterministic polynomial time Turing machine that can calculate $P'(a)$, then $\text{BQP} \subseteq \text{BPP}$.

III. PROOF

Let L be a language in the class BQP. This means that there exists a constant (error tolerance) $0 < \delta < \frac{1}{2}$, a uniform family of unitary operators $\{V_w\}$ acting on $|0\rangle^{\otimes n}$, where $n = \text{poly}(|w|)$, and a specified single qubit output register $o \in \{0, 1\}$ for the L -membership decision problem such that

1. if $w \in L$ then $\text{Prob}(o = 0) \geq 1 - \delta$ and
2. if $w \notin L$ then $\text{Prob}(o = 0) \leq \delta$.

By using the majority voting technique, δ can be exponentially small [21].

For a unitary operator V_w , we construct the DQC1 circuit of Fig. 2, where the first n -qubit Toffoli gate is defined by

$$X \otimes |0\rangle\langle 0|^{\otimes n} + I \otimes (I^{\otimes n} - |0\rangle\langle 0|^{\otimes n}),$$

and $X \equiv |0\rangle\langle 1| + |1\rangle\langle 0|$ is the bit flip operator.

For this circuit, we obtain

$$P(a = 0) = \frac{q}{2^{n-1}} + \frac{1}{2} - \frac{1}{2^n},$$

where

$$q \equiv \text{Tr} \left[\left(|0\rangle\langle 0| \otimes I^{\otimes(n-1)} \right) \left(V_w |0\rangle\langle 0|^{\otimes n} V_w^\dagger \right) \right]$$

is the probability of obtaining the positive result for the BQP circuit.

By the assumption, there exists a deterministic polynomial time Turing machine that can calculate $P'(a = 0)$. From the deterministic polynomial time Turing machine, we can construct the probabilistic polynomial time Turing machine that outputs $o \in \{0, 1\}$ according to the probability

$$\begin{aligned} \text{Prob}(o = 0) &= 2^{n-1} \left[P'(a = 0) - \frac{1}{2} + \frac{1}{2^n} \right] \\ \text{Prob}(o = 1) &= 1 - 2^{n-1} \left[P'(a = 0) - \frac{1}{2} + \frac{1}{2^n} \right]. \end{aligned}$$

Then, the probabilistic polynomial time Turing machine outputs $o = 0$ in the following way:

1. if $w \in L$ then

$$\begin{aligned} \text{Prob}(o = 0) &= 2^{n-1} \left[P'(a = 0) - \frac{1}{2} + \frac{1}{2^n} \right] \\ &\geq 2^{n-1} \left[P(a = 0) - \epsilon - \frac{1}{2} + \frac{1}{2^n} \right] \\ &= 2^{n-1} \left[\frac{q}{2^{n-1}} - \epsilon \right] \\ &= q - \epsilon 2^{n-1} \\ &\geq (1 - \delta) - \frac{1}{2^{r-(n-1)}}, \end{aligned}$$

and

2. if $w \notin L$ then

$$\begin{aligned} \text{Prob}(o = 0) &= 2^{n-1} \left[P'(a = 0) - \frac{1}{2} + \frac{1}{2^n} \right] \\ &\leq 2^{n-1} \left[P(a = 0) - \frac{1}{2} + \frac{1}{2^n} \right] \\ &= q \\ &\leq \delta, \end{aligned}$$

and therefore $\text{BQP} \subseteq \text{BPP}$.

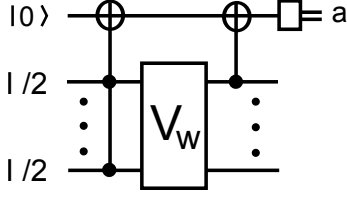


FIG. 2: The DQC1 circuit created from the n -qubit Toffoli gate and V_w .

IV. SECOND RESULT

Let us define

$$Q(a) \equiv P(a) - \frac{1}{2}.$$

The fully polynomial randomized approximation scheme (FPRAS) means that we can obtain an approximation $Q'(a)$ of $Q(a)$, which satisfies

$$\text{Prob}\left(\left|Q(a) - Q'(a)\right| \leq \epsilon Q(a)\right) \geq 1 - \eta$$

for given $\epsilon > 0$ and $0 < \eta < 1$, within $\text{poly}(\epsilon^{-1}, \ln \eta^{-1}, n)$ time.

Our second result is that if a classical computer can calculate $Q'(a)$ in the FPRAS with $\epsilon < \frac{1}{2}$ and $\eta < \frac{1}{2}$, and within $\text{poly}(n)$ time, then $\text{BQP} \subseteq \text{BPP}$. Note that $\eta = \frac{1}{4}$ is sufficient to reduce the failure probability to an arbitrarily small value η' .

V. PROOF

By the assumption, $Q'(a=0)$ can be calculated in the FPRAS. Now we can construct the probabilistic polynomial time Turing machine that outputs $o \in \{0, 1\}$ according to the probability [22]

$$\begin{aligned} \text{Prob}(o=0) &= 2^{n-1} \left[Q'(a=0) + \frac{1}{2^n} \right] \\ \text{Prob}(o=1) &= 1 - 2^{n-1} \left[Q'(a=0) + \frac{1}{2^n} \right]. \end{aligned}$$

Then, the probabilistic polynomial time Turing machine outputs $o=0$ in the following way:

1. if $w \in L$ and $Q'(a=0) \geq Q(a=0)$ then

$$\begin{aligned} \text{Prob}(o=0) &= 2^{n-1} \left[Q'(a=0) + \frac{1}{2^n} \right] \\ &\geq 2^{n-1} \left[Q(a=0) + \frac{1}{2^n} \right] \\ &= q \\ &\geq 1 - \delta. \end{aligned}$$

2. if $w \in L$ and $Q'(a=0) \leq Q(a=0)$ then [23]

$$\begin{aligned} \text{Prob}(o=0) &= 2^{n-1} \left[Q'(a=0) + \frac{1}{2^n} \right] \\ &\geq 2^{n-1} \left[(1 - \epsilon)Q(a=0) + \frac{1}{2^n} \right] \\ &= (1 - \epsilon)q + \frac{\epsilon}{2} \\ &\geq (1 - \epsilon)(1 - \delta) + \frac{\epsilon}{2} \\ &\geq (1 - \epsilon)(1 - \delta). \end{aligned}$$

3. if $w \notin L$ and $Q'(a=0) \leq Q(a=0)$ then

$$\begin{aligned} \text{Prob}(o=0) &= 2^{n-1} \left[Q'(a=0) + \frac{1}{2^n} \right] \\ &\leq 2^{n-1} \left[Q(a=0) + \frac{1}{2^n} \right] \\ &= q \\ &\leq \delta. \end{aligned}$$

4. if $w \notin L$ and $Q'(a=0) \geq Q(a=0)$ then [23]

$$\begin{aligned} \text{Prob}(o=0) &= 2^{n-1} \left[Q'(a=0) + \frac{1}{2^n} \right] \\ &\leq 2^{n-1} \left[(1 + \epsilon)Q(a=0) + \frac{1}{2^n} \right] \\ &= (1 + \epsilon)q - \frac{\epsilon}{2} \\ &\leq (1 + \epsilon)\delta - \frac{\epsilon}{2} \\ &\leq (1 + \epsilon)\delta. \end{aligned}$$

Therefore we conclude that $\text{BQP} \subseteq \text{BPP}$.

VI. DISCUSSION

In this paper, we have shown that the classical efficient approximation (exactly within a polynomial bit length or in the FPRAS with at most a constant error) of the output probability distribution of the DQC1 model is impossible unless $\text{BQP} \subseteq \text{BPP}$. Since it is believed that $\text{BPP} \subsetneq \text{BQP}$, our results suggest that it is unlikely that the DQC1 model can be simulated in these senses.

In Ref. [10], it was shown that the DQC1 model cannot be simulated by using the tensor-network method, since the Schmidt rank increases exponentially. Our first result can be considered as a generalization of their result: whatever method is utilized, classical efficient simulation of the DQC1 model is impossible (unless $\text{BQP} \subseteq \text{BPP}$).

As we have mentioned, our definitions of classical simulatability are stronger than the sampling considered in Refs. [12, 16]. It will be a future study to generalize our results to the sampling.

Acknowledgments

TM is supported by the Tenure Track System by MEXT Japan and KAKENHI 26730003 by JSPS. TK is

supported by KAKENHI 26540002, 24106008, 24240001, 23246071 by JSPS.

-
- [1] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
 - [2] A. Ambainis, L. J. Schulman, and U. V. Vazirani, Proc. of the 32nd Ann. ACM Sympo. on Theor. of Comput. pp. 697 (2000).
 - [3] D. Poulin, R. Laflamme, G. J. Milburn, and J. P. Paz, Phys. Rev. A **68**, 022302 (2003).
 - [4] D. Poulin, R. Blume-Kohout, R. Laflamme, and H. Olivier, Phys. Rev. Lett. **92**, 177906 (2004).
 - [5] P. W. Shor and S. P. Jordan, Quant. Inf. Comput. **8**, 681 (2008).
 - [6] S. P. Jordan and P. Wocjan, Quant. Inf. Comput. **9**, 264 (2009).
 - [7] G. Passante, O. Moussa, C. A. Ryan, and R. Laflamme, Phys. Rev. Lett. **103**, 250501 (2009).
 - [8] S. P. Jordan and G. Alagic, Proc. of the Sixth Conference on Theory of Quantum Computation, Communication and Cryptography (TQC 2011); arXiv:1105.5100
 - [9] A. Datta, A. Shaji and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).
 - [10] A. Datta and G. Vidal, Phys. Rev. A **75**, 042310 (2007).
 - [11] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A **72**, 042316 (2005).
 - [12] T. Morimae, K. Fujii, and J. F. Fitzsimons, Phys. Rev. Lett. **112**, 130502 (2014).
 - [13] T. Kapourniotis, E. Kashefi, and A. Datta, arXiv:1403.1438
 - [14] S. Toda, SIAM J. Comput. **20**, 865 (1991).
 - [15] B. Terhal and D. DiVincenzo, Quant. Inf. Comput. **4**, 134 (2004).
 - [16] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. R. Soc. A **467**, 2126 (2011).
 - [17] S. Aaronson and A. Arkhipov, Theory of Computing **9**, 143 (2013).
 - [18] E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997).
 - [19] D. Gottesman, arXiv:9807006
 - [20] D. DiVincenzo and B. Terhal, arXiv:0403031.
 - [21] S. Arora and B. Barak, *Computational complexity: a modern approach* (Cambridge University Press 2009)
 - [22] If $Q'(a=0) \leq Q(a=0)$, $2^{n-1}[Q'(a=0) + \frac{1}{2^n}] > 1$ cannot be happen since $2^{n-1}[Q'(a=0) + \frac{1}{2^n}] \leq 2^{n-1}[Q(a=0) + \frac{1}{2^n}] = q$. If $Q'(a=0) \geq Q(a=0)$, and $2^{n-1}[Q'(a=0) + \frac{1}{2^n}] > 1$, we set $Prob(o=0) = 1$, since in this case $2^{n-1}[Q'(a=0) + \frac{1}{2^n}] > 1$ means $q > \frac{2}{3} > \frac{1}{2}$.
 - [23] Note that this inequality is not satisfied with the small failure probability η' due to the definition of FPRAS. However, it does not affect the result.